PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04Q 7/22, H04L 29/06

A1

(11) International Publication Number: WO 99/33291

(43) International Publication Date: 1 July 1999 (01.07.99)

(21) International Application Number: PCT/SE98/02322

(22) International Filing Date: 15 December 1998 (15.12.98)

(30) Priority Data:
08/995,170 19 December 1997 (19.12.97) US

(71) Applicant: TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventors: KARLSSON, Torgny; Beckombergavägen 13, 4409, S-168 54 Bromma (SE). HERLITZ, Anders; Edinsvägen 8 2tr ned, S-131 45 Nacka (SE).

(74) Agent: ERICSSON RADIO SYSTEMS AB; Common Patent Dept., S-164 80 Stockholm (SE).

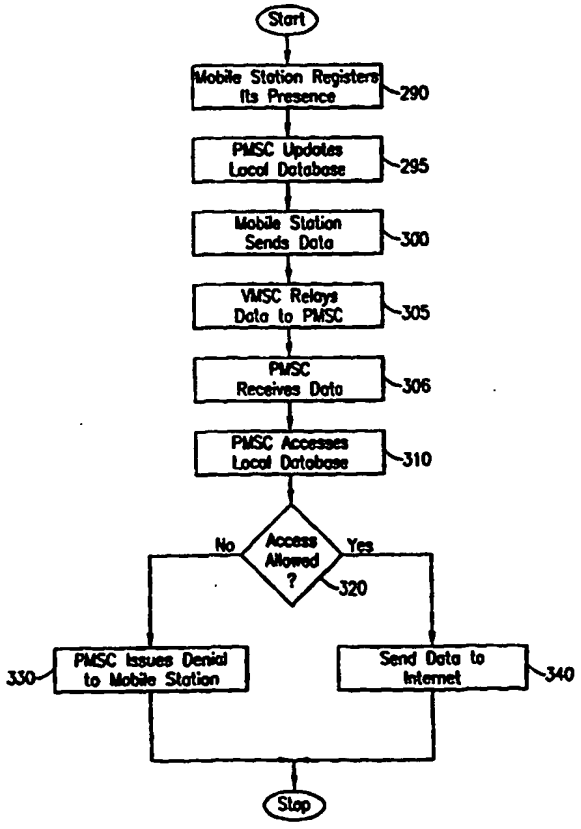
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: INTERNET PROTOCOL TRAFFIC FILTER FOR A MOBILE RADIO NETWORK

(57) Abstract

An Internet Protocol traffic filter is provided for a mobile radio network (100). A database (211) stores access privileges of the mobile station (150) for accessing a remote host (130), and access privileges of the remote host (130) for accessing the mobile station (150). A processor (210) receives (306) data from the mobile station (150) addressed to a remote host (130). The processor (210) accesses (310) the database (211) to determine (320) whether the mobile station (150) is allowed to access the remote host (130), and denies (330) access if access is unauthorized. Otherwise, the processor (210) sends (340) the data to the remote host (130) if access is authorized. The processor (210) also receives (420) data from a remote host (130), and determines (440) whether the remote host (130) is allowed to access the mobile station (150). The processor (210) denies (450) access to the mobile station (150) if the remote host (130) is unauthorized. Otherwise, the processor (210) connects (460) the remote host (130) to the mobile station (150) if access is authorized.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

INTERNET PROTOCOL TRAFFIC FILTER FOR A MOBILE RADIO NETWORK

BACKGROUND OF THE INVENTION

Technical Field of the Invention

The present invention pertains in general to a method and apparatus for filtering data packets transmitted across a communication network and, more particularly, to a method and apparatus for filtering the transmission of data packets between a mobile station in a mobile radio network and an Internet Protocol (IP) type network.

Description of the Related Art

Packet data services are being introduced at an increasing rate into mobile radio networks. Packet data services provide an efficient connection between digital terminal equipment connected to mobile stations in a mobile radio network and remote hosts connected to the Internet. Using a packet data service, data is transmitted between the remote host and the digital terminal equipment as discrete data packets. The use of discrete data packets allows a mobile radio network operator to convey data from several mobile stations on a single channel and, further, to charge mobile station subscribers based on the quantity of data transmitted across the mobile radio network rather than on the duration of a connection between the mobile station and the remote host.

Using the packet data service, the mobile station subscriber connects digital terminal equipment, such as a personal computer, to the Internet or an Internet-like network such as an Intranet. This allows the mobile station subscriber to access remote hosts on the Internet and, in turn, allows remote hosts on the Internet to access the digital terminal equipment connected to the mobile station. For various reasons, mobile station subscribers and the mobile radio network operator may desire to control the flow of the IP traffic both to and from the mobile station. For example, since the mobile station subscriber is charged for data packets sent to the mobile station

subscriber by a remote host, the mobile station subscriber may wish to filter IP traffic directed to the digital terminal equipment to certain authorized remote hosts.

In a similar fashion, the mobile radio network operator may wish to individually filter the ability of each mobile station to access remote hosts. For example, the mobile radio network operator may wish to create a virtual network, wherein a select group of mobile station subscribers and remote hosts have access to the virtual network. By establishing such virtual networks, the mobile radio network operator can charge different tariffs to each mobile station subscriber based on the subscriber's membership in one or more of the virtual networks.

Several techniques currently exist for controlling the transmission of data between computing devices over a network. These techniques apply both to hosts on the same network as well as to hosts located on different networks. For example, firewalls are commonly used as barriers between an internal network and external hosts to prevent the internal network from unauthorized access by the external hosts or others. The firewall also prevents the transmission of data from the external host to hosts on the internal network.

Other techniques for filtering traffic on a communication network involve filtering the communication of data to certain segments of a single or multiple communication networks. Such techniques are based on the address of the destination host and apply indiscriminately to all hosts. These filtering techniques are designed to increase the bandwidth of the communication network by filtering communication of the data to only those segments of the communication network necessary for the data to reach the destination host from the originating host.

It would be advantageous to devise a method and apparatus to individually filter IP traffic for each mobile station in a mobile radio network so as to filter communication between digital terminal equipment connected to a mobile station on a mobile radio network and remote hosts located on an Internet. It would also be advantageous if such a method and apparatus allowed both the mobile station subscriber and the mobile radio network operator to independently establish access privileges to and from the digital terminal equipment.

SUMMARY OF THE INVENTION

The present invention comprises an IP traffic filter for a mobile radio network. A database stores access privileges for the mobile station to access a remote host, and access privileges for the remote host to access the mobile station. A processor receives data from the mobile station addressed to a remote host. The processor accesses a local copy of the database to determine whether the mobile station is allowed to access the remote host, and denies access if access to the remote host by the mobile station is unauthorized. Otherwise, the processor allows access to a remote host if access to the remote host is authorized.

The processor also receives data from a remote host addressed to the mobile station, and determines whether the remote host is allowed to access the mobile station. The processor denies access to the mobile station if the remote host is unauthorized. Otherwise, the processor allows the remote host to access the mobile station if access to the mobile station by the remote host is authorized.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention, reference is made to the following detailed description taken in conjunction with the accompanying drawings wherein:

FIGURE 1 is a functional block diagram of an IP traffic filter for a mobile radio network consistent with a preferred embodiment of the present invention;

FIGURE 2 is a flow diagram of a method for filtering access to a remote host by a mobile station consistent with the preferred embodiment of the present invention; and

FIGURE 3 is a flow diagram of a method for filtering access to digital terminal equipment connected to a mobile station by a remote host consistent with the preferred embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

Referring now to Figure 1, there is illustrated a functional block diagram of an IP traffic filter consistent with a preferred embodiment of the present invention. A mobile radio network 100 communicates with an Internet 110 via a router 120. The

mobile radio network 100 can be any type of mobile radio network, such as, for example, a cellular telephone network, and can be implemented using any appropriate architecture or air interface standard. For illustrative purposes, the mobile radio network 100 is described as implementing a Personal Digital Cellular (PDC) protocol. Likewise, the Internet 110 can be any type of network following IP standards. The Internet 110 is connected to one or more remote hosts 130. Digital terminal equipment 140, such as a personal computer, communicates with the remote host 130 via a mobile station 150, and the mobile station 150 communicates with a base station 160 of the mobile radio network 100 via an air interface 170.

For voice communication, the base station 160 communicates with the mobile radio network 100 through a Visited Mobile services Switching Center (VMSC) 180 via a speech communication link 190. For data communications, the base station 160 communicates with a Packet Mobile services Switching Center (PMSC) 210 through the VMSC 180 via a packet data service link 200. The PMSC 210 is responsible for handling data packets communicated to and from the digital terminal equipment 140.

The PMSC 210 communicates with the Internet 110 via the router 120. Information regarding the access privileges of the mobile station 150 and the remote host 130 are stored in a database located in a Home Location Register (HLR) 220. The PMSC 210 maintains a local copy 211 of access privileges contained in the HLR 220 for all mobile stations 150 which have registered their presence in the mobile radio network 100. The data contained in the databases can be entered or modified by the mobile radio operator via the operation center 240. The data contained in the databases can also be entered or modified by the mobile station subscriber. As an example, the user interface for the subscriber can be a web server accessible from the Internet 110 and provides a service for entering and modifying filter parameters. Operation of the base station 160, the VMSC 180 and the HLR 220 to effectuate voice communication between the mobile station 150 and the mobile radio network 100, is performed by conventional methods. Likewise, data packet communication between digital terminal equipment 140 and remote hosts 130 is performed by conventional methods.

The databases located in the HLR 220 and the local copy 211 store information associated with the mobile station 150 identifying which remote hosts 130 the mobile station 150 is allowed to access. The databases also contain information identifying which remote hosts 130 are allowed to access the mobile station 150. The data contained in the databases can be entered or modified by the mobile radio operator via the operation center 240. The data contained in the databases can also be entered or modified by the mobile station subscriber. As an example, the user interface for the subscriber can be a web server accessible from the Internet 110 and provides a service for entering and modifying filter parameters.

Referring now to Figure 2, there is illustrated a method for filtering IP traffic. When a mobile station 150 initiates operation in the mobile radio network 100, the mobile station 150 registers its presence with the mobile radio network 100 (step 290) and in response the PMSC 210 updates the local database 211 (step 295). The computing device 140 sends data to a remote host 130(step 300) and the data is relayed through the VMSC 180 to the PMSC 210 (step 305). The PMSC 210 receives the identity of the mobile station 150 included with the data which, in this exemplary embodiment, is a mobile station International Mobile Station Identity (IMSI) number associated with the mobile station 150. The PMSC 210 also receives an IP address associated with the mobile station 150 and the digital terminal equipment 140, as well as the IP address of the remote host 130 (step 306). The PMSC 210 accesses the local database 211 to determine the access privileges of the mobile station 150 to access the remote host 130 (step 310). The database in the HLR 220 and the local database 211 contain a list of allowed remote hosts 130 associated with the mobile station 150 or, in an alternative, the databases contain a list of disallowed remote hosts 130 associated with the mobile station 150. In any event, the PMSC 210 receives the information and determines whether the mobile station 150 is authorized to access the remote host 130 based on the information contained in the local database 211(step 320). In another embodiment of the present invention, the database in the HLR 220 and the local database 211, group the mobile station 150 and the remote hosts 130 into one or more virtual networks. Access to the remote host 130 from the mobile station 150, as well as access from the remote host 130 to the mobile station 150, is based on membership in a particular virtual network.

After determining the access rights of the mobile station 150 in step 320, the PMSC 210 either allows, or denies access based on the determination. If the PMSC 210 has determined that access is not allowed, the PMSC 210 issues a denial message to the mobile station 150 (step 330). Otherwise, if the PMSC 210 determines that access is allowed, the PMSC 210 continues sending the data to the Internet 110 (step 340). The PMSC 210 sends data to the Internet 110 via the router 120 in a conventional manner.

Referring now to Figure 3, there is illustrated a flow diagram of a method for filtering requests to digital terminal equipment connected to a mobile station by a remote host consistent with the preferred embodiment of the present invention. When a mobile station 150 initiates operation in the mobile radio network 100, the mobile station 150 registers its presence with the mobile radio network 100 (step 390) and in response the PMSC 210 updates the local database 211 (step 395). The remote host 130 sends a data packet to the PMSC 210(step 400) via the Internet 110 and the router 120. The router 120 receives the data and relays the data to the PMSC 210 (step 410). The PMSC 210 receives the data (step 420) and accesses the local database 211 (step 430). The PMSC 210 uses the information contained in the database to determine whether access by the remote host 130 to the digital terminal equipment 140 connected to the mobile station 150 is allowed (step 440). If access is not allowed, the PMSC 210 issues a denial to the remote host 130 (step 450). Otherwise, the PMSC 210 sends the data to the digital terminal equipment 140 connected to the mobile station 150 via the mobile radio network 100 (step 460).

Storing the data pertaining to access privileges in the HLR 220 enables the use of current roaming functions which are well known in the industry. This allows subscribers to roam between different mobile radio networks and with the access privileges data remaining valid

Although a preferred embodiment of the method and apparatus of the present invention has been illustrated in the accompanying Drawings and described in the foregoing Detailed Description, it is understood that the invention is not limited to the embodiment disclosed, but is capable of numerous rearrangements, modifications, and substitutions without departing from the spirit of the invention as set forth and defined by the following claims.

WHAT IS CLAIMED IS:

1. An IP traffic filter for a mobile radio network comprising:

a database for storing access privileges of a mobile station for accessing a remote host, and access privileges of said remote host for accessing said mobile station; and

a processor for routing data to and from said mobile station, the processor further for accessing said database to determine access privileges, and for denying or allowing access in response to a determined access privilege.

2. The IP traffic filter of Claim 1, wherein said processor comprises a PMSC in said mobile radio network.

3. The IP filter recited of Claim 1, further comprising a HLR for maintaining said database.

4. The IP filter recited in Claim 1, further comprising a router for connecting said mobile radio network to an Internet.

5. The IP filter recited in Claim 1, further comprising a means for entering and modifying data said database.

6. The IP filter recited in Claim 5, wherein said means for entering and modifying data in said database comprises an Internet web server.

7. A method for filtering IP traffic originating from a mobile station in a mobile radio network, comprising the steps of:

receiving data from said mobile station to addressed to a remote host;

determining access rights of said mobile station to access said remote host;

denying access to said remote host if said access is unauthorized; and

forwarding said data to said remote host if said access is authorized.

8. The method of Claim 7, wherein the step of receiving data addressed to said remote host comprises the steps of:

receiving an identity of the said mobile station;

receiving an IP address of said remote host; and

receiving an IP address associated with said mobile station.

9. The method of Claim 8, wherein the step of receiving said identity of said mobile station comprises receiving an IMSI number associated with said mobile station.

10. The method of Claim 8, wherein the step of determining access rights of said mobile station comprises comparing the IP address of said remote host against a list of allowed destination hosts associated with said mobile station.

11. The method of Claim 8, wherein the step of determining access rights of said mobile station comprises comparing said IP address of said remote host against a list of disallowed destination hosts associated with said mobile station.

12. The method of Claim 8, wherein the step of determining access rights of said mobile station comprises comparing the IP address of said remote host and said identity of said mobile station against membership in a virtual network.

13. A method for filtering IP traffic directed to a mobile station in a mobile radio network from a remote host comprising the steps of:

receiving data addressed to said mobile station;

determining access rights of said remote host;

denying access to said mobile station if access to said mobile station by said remote host is unauthorized; otherwise

sending data from said remote host to said mobile station if said access to said mobile station by said remote host is authorized.

14. The method of Claim 13, wherein the step of determining said access rights of said remote host comprises comparing said IP address of said remote host against a list of allowed originating remote hosts associated with said mobile station.

15. The method of Claim 13, wherein the step of determining said access rights of said remote host comprises comparing said IP address of said remote host against a list of disallowed originating remote hosts associated with said mobile station.

16. The method of Claim 13, wherein the step of determining said access rights of said remote host comprises comparing said IP address of said remote host and said identity of said mobile station against membership in a virtual network.

17. The method of Claim 13, wherein the step of denying access to said mobile station comprises transmitting a denial message to said remote host.

18. The method of Claim 13, wherein the step of determining said access rights of said remote host further comprises converting said IP address of said mobile station to an associated mobile station ISDN number.

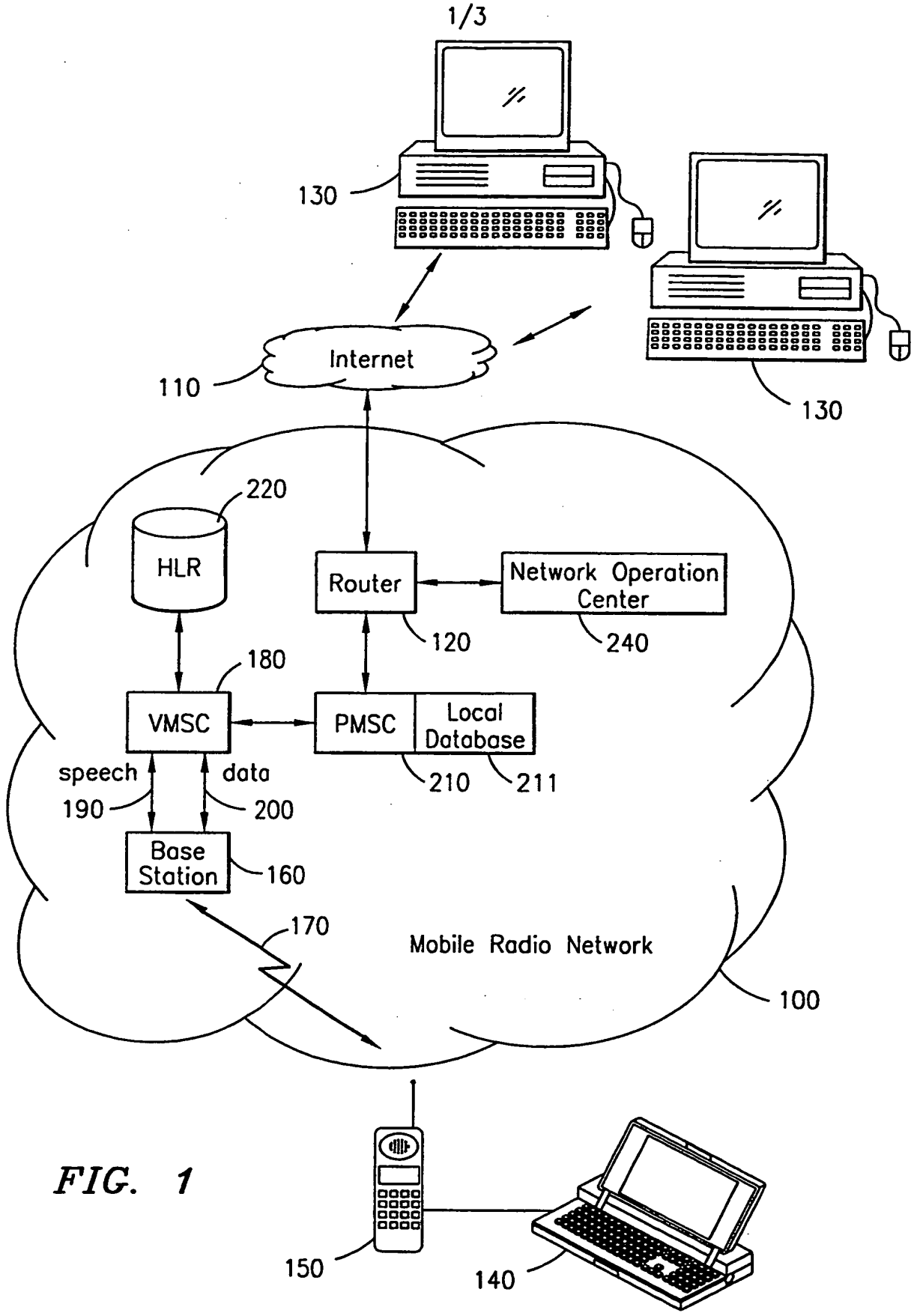


FIG. 1

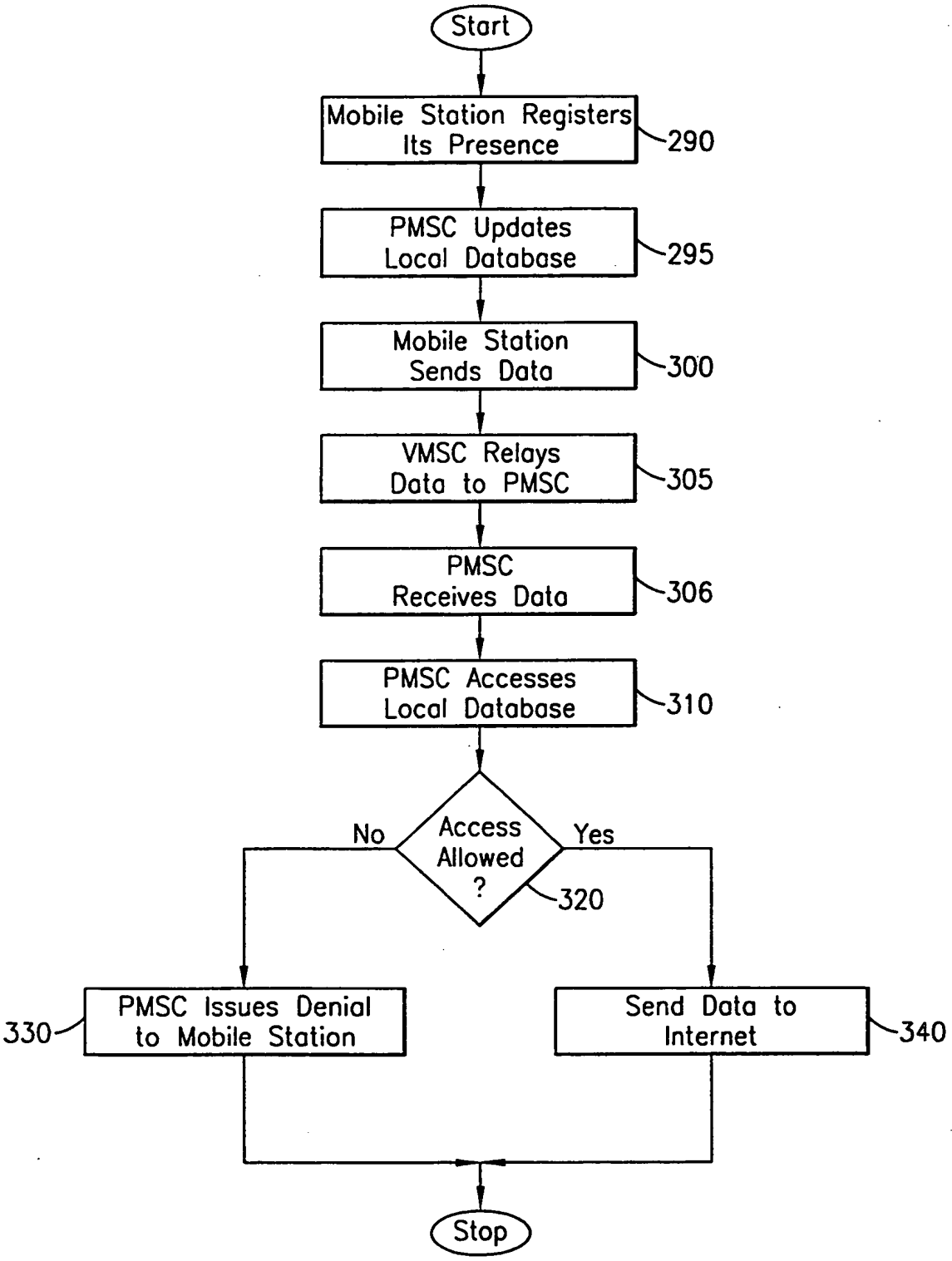


FIG. 2

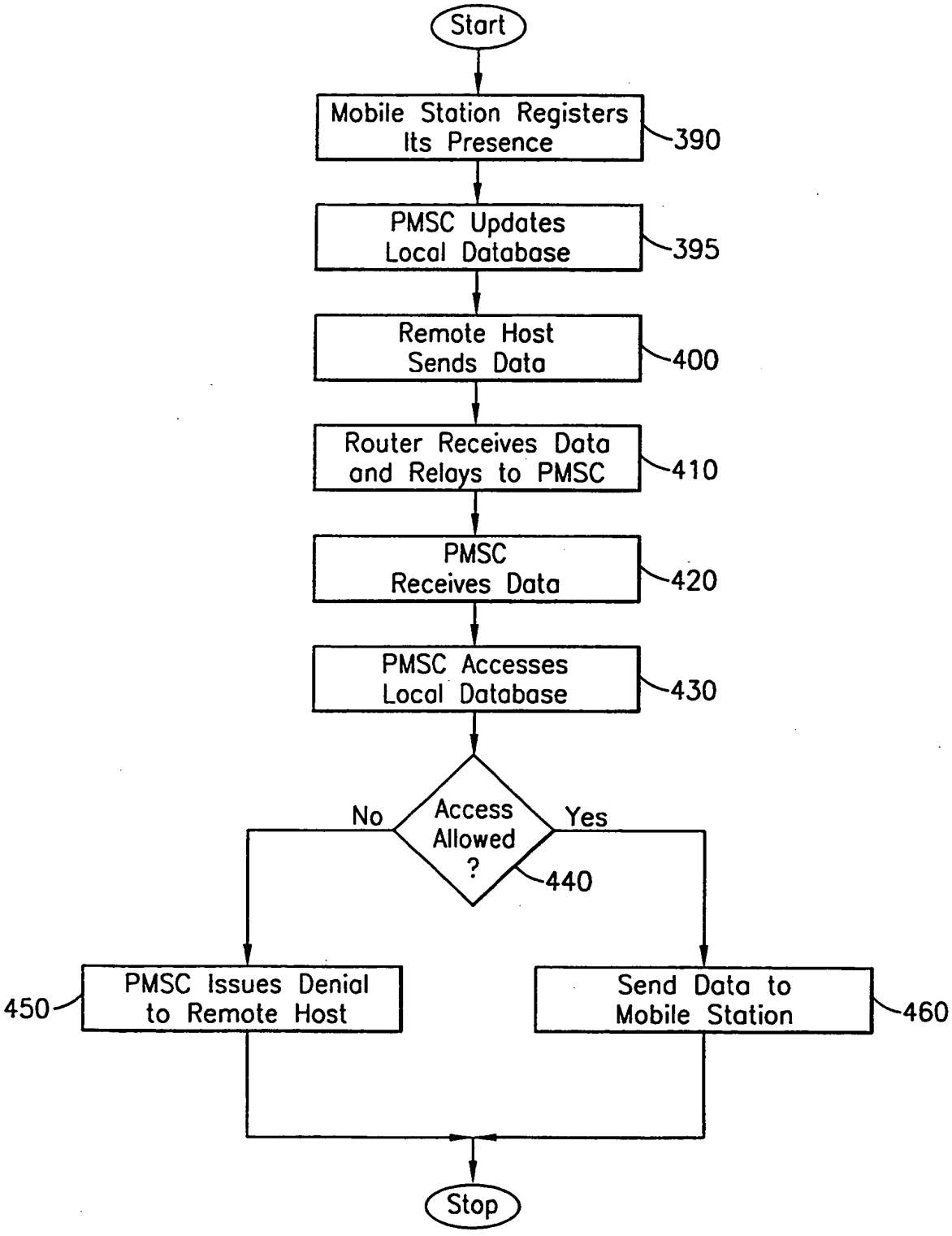


FIG. 3

INTERNATIONAL SEARCH REPORT

Interr nal Application No
PCT/SE 98/02322

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04Q7/22 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04Q H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	BELLOVIN S M ET AL: "NETWORK FIREWALLS" IEEE COMMUNICATIONS MAGAZINE, vol. 32, no. 9, 1 September 1994, pages 50-57, XP000476555 see page 51, right-hand column, line 56 - page 52, right-hand column, line 35 --- -/--	1-18

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 April 1999	28/04/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Roberti, V

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/SE 98/02322

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SUGIYAMA K ET AL: "PACKET ROUTING FUNCTION ON THE PDC MOBILE PACKET DATA COMMUNICATIONNETWORK" 1996 IEEE INTERNATIONAL CONFERENCE ON COMMUNICATIONS (ICC), CONVERGING TECHNOLOGIES FOR TOMORROW'S APPLICATIONS DALLAS, JUNE 23 - 27, 1996, vol. VOL. 3, 23 June 1996, pages 1382-1385, XP000625036 INSTITUTE OF ELECTRICAL & ELECTRONICS ENGINEERS see the whole document ---	1-18
A	EP 0 812 085 A (NIPPON TELEGRAPH & TELEPHONE) 10 December 1997 see page 5, line 13 - page 13, line 9 ---	1-18
A	EP 0 658 837 A (CHECKPOINT SOFTWARE TECHN LTD) 21 June 1995 see page 3, line 36 - page 4, line 15 see page 4, line 54 - page 5, line 3 see page 6, line 22 - page 7, line 2 -----	1-18

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Interr nal Application No
PCT/SE 98/02322

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0812085 A	10-12-1997	AU 1171797 A	17-07-1997
		WO 9723977 A	03-07-1997
EP 0658837 A	21-06-1995	US 5606668 A	25-02-1997
		CA 2138058 A	16-06-1995
		WO 9700471 A	03-01-1997
		JP 8044642 A	16-02-1996
		US 5835726 A	10-11-1998